

ADVISORY REPORT

Implementing signature verification systems to help enable operational flexibility and improve fraud detection.

Despite the emergence of electronic banking, millions of check and other paper-based transactions are processed every day, requiring signature verification to authenticate the transaction and prevent fraud. Implementing a signature verification system can help enable operational flexibility and improves fraud detection.

Based on Unisys experience, this paper highlights the key considerations when planning the implementation of a signature verification system.

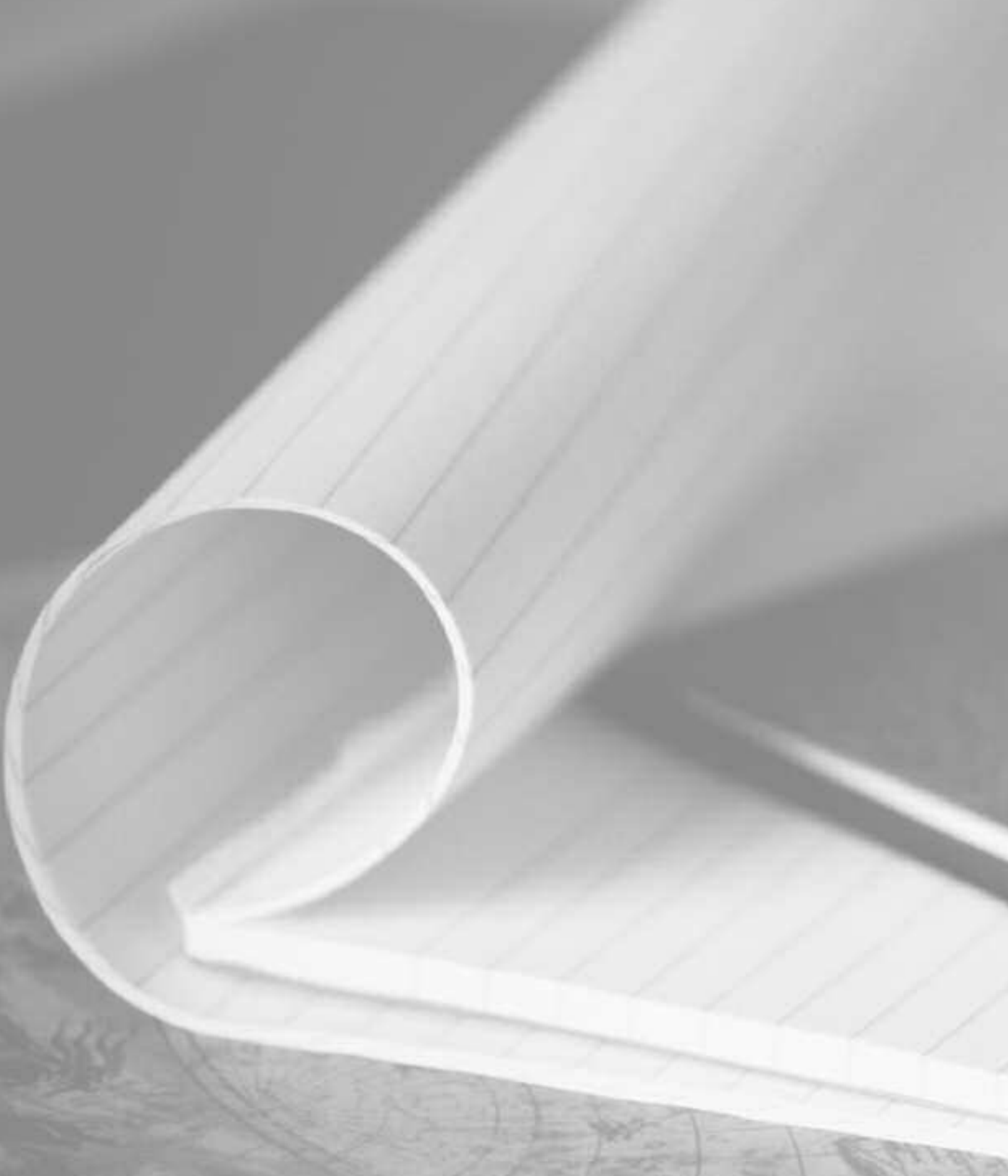
COMBATTING
IDENTITY FRAUD.

IMAGINE IT.

- > Consulting.
- > Systems Integration.
- > Outsourcing.
- > Infrastructure.
- > Server Technology.

UNISYS

Imagine it • Done •



Despite the trends heralding electronic banking, millions of paper-based transactions are still processed every day. In the back office, high-value check payments and other instructions—such as change of address, amendments to account signatories, standing orders and direct debits—remain a potential source of fraud and require authentication before being executed.

The only authorization for these transactions is to verify the signature against a reference signature. Signing rules may also need to be verified; these may range from a simple “one or both to sign” for a joint personal account to complex rules associated with major corporate accounts.

Check fraud and identity theft are two challenges facing banks today:

- ▶ In the U.K., APACS noted that “The Company is aware of the potential for increased check fraud as security on other payment methods is upgraded. Recent statistics show that incidents of counterfeit, as well as fraudulent alteration of amount and payee details, are increasing substantially, with fraudsters focusing on identity fraud and improved-quality counterfeiting.”¹

APACS reported that in 2003, 41,000 cheques were forged, counterfeit or altered, creating a potential loss of £566m. While many instances of cheque fraud were foiled, actual losses still topped £45m—up 50% on 2002. In the first six months of 2004, cheque fraud exceeded £24m and the total for the year is expected to significantly exceed the figure for 2003.

- ▶ Fraud is a significant concern to bank branch customers today—a concern that can translate into considerable lost revenue for banks: Nearly half of all U.S. bank customers would be willing to switch to a bank that offered identity theft detection and alert services, according to the results from a two-part Unisys study.

The research analyzed consumer perceptions of identity theft, and how bank personnel address the issue.²

- ▶ In 2001, check fraud losses in the U.S. banking industry amounted to \$698m. 24% of these losses were due to forged signatures.³

Signature verification remains a key defense in the fight against fraud.

Signature verification.

Historically, signature verification was handled at the branch, where reference documents are stored in back-office filing cabinets. Many institutions have centralized back-office processing into service centers, and increasing volumes of transactions are being processed offshore. At the same time, transactions initiated by customers in the branch network must also be authenticated.

To provide the operational flexibility required and to maintain customer service, banks today need ready access to reference signatures at multiple locations. Reliance on paper-based records constrains any form of centralization without incurring significant clerical overhead or payment risk. Storage of documents and access to reference signatures require significant overhead, productivity suffers and face-to-face transactions become increasingly protracted.

Today’s best-of-breed solutions address these issues and can help achieve operational flexibility, increased fraud detection and improved customer service.

This white paper provides a broad overview of the key considerations that banks must take into account when planning the implementation of a signature-verification system.

¹APACS Annual Review 2003, APACS, March 2004.

²Identity Theft Prevention and Detection: Are Your Branch Banking Customers at Risk? Unisys, 2005.

³2001 fraud survey of 439 banks, conducted by the American Bankers Association, published in *Banking Strategies*, March/April 2003.



Signature verification systems.

Signature-verification systems have been available since the 1980s. However, not all meet the needs of the 21st century bank. Limitations may include:

- ▶ Narrowly focused implementations that are limited to specific market sectors (such as business accounts) or processes (such as check-signature verification)
- ▶ Limited capability for integration with other systems, including workflow solutions, fraud detection and customer information
- ▶ Lack of support for easy enterprise-wide deployment
- ▶ Inability to support “off-shore” processing due to limited availability
- ▶ Insufficient resiliency for a mission-critical system
- ▶ Data maintenance issues that reduce the integrity of the information stored.

Mergers and acquisitions often result in disparate systems that remain in use post-merger, with the associated duplication in infrastructure and support costs.

Enhancements to signature verification systems hold promise for the banking industry to further improve processing. Future-proofed solutions are available today that incorporate Automated Signature Verification and Biometric Signature Verification.

Automatic signature verification (ASV).

ASV incorporates an image-based workflow into the verification process, automatically comparing signatures on paper-based transactions with specimen signatures stored in the system. This results in improved accuracy and consistency.

In the U.S., it has been reported that “... criminals have reduced the amounts of their fraudulent checks to avoid detection, a response to the fact that banks prioritize fraud investigation on checks over a certain limit.”⁴ Implementing ASV offers banks the option of comparing signatures on low value items whilst specialists focus solely on the most questionable items.

⁴*Banking Strategies, March/April 2003, p. 30.*

Biometric signature verification.

In addition to authenticating using the visual appearance, a signature can be authenticated by comparing other characteristics such as the pressure applied while signing, and the speed at which the signature is written. Because they make every signature as unique as a fingerprint, such biometrics can be used to further improve fraud detection. Tablet PCs or pressure-sensitive pen pads can capture the reference signature and provide on-the-spot authentication.

Today's requirements.

Many organizations are reviewing their signature verification processes and systems to increase operational efficiency and improve fraud detection. Newer systems have features that facilitate such efficiencies by:

- ▶ Allowing processes to be located where most appropriate, with the flexibility to change in the future
- ▶ Automating manual signature-verification processes
- ▶ Providing a balanced view of risk
- ▶ Ensuring enterprise-wide data consistency
- ▶ Integrating with other fraud-detection systems where necessary
- ▶ Establishing a platform for future enhancement.

Benefits.

The primary driver for implementing a signature verification system is often to enable operational flexibility whilst maintaining fraud detection processes—paper-based transactions can be processed at any location. Other benefits can also be realized by improving the signature verification process, including:

- ▶ Reduction in signature verification costs for check and other paper transactions by using images instead of paper-based records.



- ▶ Improving the end-to-end process by integrating the signature verification and workflow systems.
- ▶ Reducing infrastructure costs by moving document hard copies into deep storage.
- ▶ Enhanced fraud detection.
- ▶ Improved customer service.

Additionally, “soft” benefits can be gained, such as a major improvement in data quality. Accurate, consistent and up-to-date data for accounts—including an audit trail of updates—can be made available throughout the enterprise.

Signature-verification systems also provide the opportunity to further improve fraud detection by using ASV and biometric signature verification, in addition to visual verification techniques.

Costs.

Three major cost elements when implementing a signature-verification system are:

- ▶ System implementation
- ▶ Initial database population (back-file conversion)
- ▶ On-going database maintenance.



While addressing these cost factors, the organization must understand the business requirements, identify opportunities for process re-engineering, review options for minimizing costs, and consider alternative implementation approaches.

System implementation.

Business requirements.

Developing a clear understanding of the intended verification processing is one key factor in determining the solution requirements.

Key considerations include:

- ▶ Which paper transactions will be verified?
- ▶ Where will these transactions be verified?
- ▶ Which verification techniques will be used?
- ▶ How many transactions will be verified?
- ▶ How many users will require access to the system?
- ▶ Will “on demand” availability of signatures generate additional usage?
- ▶ Which customer information, payment and fraud systems must integrate with the signature verification system?

Identifying which transactions will be verified establishes which legacy and new workflow systems must be integrated with the signature-verification solution.

Understanding where transactions will be verified determines a deployment approach. For example, access from a large branch network for face-to-face authentication may best be achieved through the use of browser-based solutions.

Understanding the volumes, the number of users, and the availability and disaster-recovery requirements will ensure the system is sized correctly. For example, access from offshore processing sites requires that the system be available for longer periods than would otherwise be the case.

If the requirement includes the implementation of ASV or biometric verification, the incremental costs for this solution must be included.

Build or buy?

When implementing a signature and mandate database, “build or buy?” becomes a key decision. Today’s leading software packages have overcome the limitations of earlier systems. A fully featured application should offer the following functionality:

- ▶ Support for ASV and/or biometric signature verification for initial or future deployment
- ▶ A thin-client interface to ease deployment throughout the branch network and other delivery channels
- ▶ Integration with legacy and new workflow systems and with customer information systems
- ▶ Support for the required volume of concurrent users and transactions.

IT outsourcing.

A signature verification system must provide high levels of accessibility with strict service levels for availability and reliability. The hosting of such a system is a candidate for IT Outsourcing from ITO provider with a track record in meeting strict SLAs.

Back-File conversion.

Historically, the implementation starts by acquiring images of signatures from mandates and signature cards.

The initial population of the database may represent a significant percentage of the overall implementation costs. Developing a clear strategy for the initial population of the database will ensure that schedules and costs for this exercise are accurately estimated.

To minimize these costs, consider the following:

- ▶ Electronic conversion from existing systems to automate database population
- ▶ The most efficient processes for paper-to-image conversion to complete database population for accounts with signatures that are not populated automatically; understanding the current manual process can help determine the optimal approach to extraction and scanning
- ▶ Outsourcing some or all of the back-file conversion.

By investing time early in the project to identify the optimal strategy, banks can minimize the significant costs associated with the initial population and ensure that realistic costs are included in the business case.

Electronic conversion.

Automated conversion is the primary approach when migrating images and data from legacy signature database systems and document imaging systems.

This approach also can minimize the costs associated with a primarily manual back file conversion. “In-flight capture” scans and stores signatures from checks as they are processed by clearing systems; the signatures are stored in a temporary repository and, after validation, are used to populate the database.

Other potential sources include microfilm and microfiche that contain images of mandates and signature cards.

When investigating these approaches, be sure to confirm that the quality of the images from the source systems is sufficient for the purpose. For example, ASV requires signatures to be imaged at a higher resolution than that required for visual verification.

If suitable images exist in document imaging systems, it may be possible to extract the necessary signature characteristics from images using ink-layer analysis techniques to enable biometric signature verification.

Paper-to-Image conversion.

Even using the techniques described above, a significant volume of paper records will likely need to be located, extracted and scanned to complete the population of the database.

Two approaches can be taken for converting paper records to digital images:

- ▶ Documents can be scanned “in-situ” by roving teams equipped with notebook PCs and document scanners
- ▶ Documents can be transported to a centralized scanning and data-entry facility.

Regardless of the approach, it is important to have a good understanding of the quality (completeness and accuracy) of the source documents and their filing systems. To determine the level of document preparation required to ensure an efficient scanning and data entry exercise, a bank must answer questions such as:

- ▶ Are documents filed alphabetically (by name) or numerically (by account number)?
- ▶ Is the same order used at each site where documents are stored?
- ▶ How reliable is the order in which documents are filed?
- ▶ How many different formats of documents have been introduced? Are there other papers stored with the documents that need to be scanned?



- ▶ Are redundant documents removed from the filing system?
- ▶ What proportion of documents is expected to be missing?

Additionally, you must analyze the source documents to determine whether they are suitable for imaging.

Business process outsourcing.

Depending on the volume of paper records to be scanned and the time period available for the initial population of the database, a large team may be required. Because this team—and some of their technology support—will only be required for a relatively short period of time, the initial population of the database is a process that is an ideal candidate for Business Process Outsourcing (BPO), alleviating the need to recruit, equip and train the team.

Database maintenance.

As soon as the back-file conversion has commenced, it is essential to keep the database up to date with details of new, changed and closed accounts.

The variable costs associated with database maintenance are driven by the volume of maintenance. When estimating volumes, be sure to consider both account closures and account openings. Other significant cost drivers that may be overlooked are changes to account signatories such as marriage and change of signing officials. Understanding these considerations will help identify the true maintenance volumes that will have to be processed on a regular basis.

Maintenance costs can be minimized by designing an efficient process:

- ▶ Signature cards and mandate forms can be re-designed so that the forms or “tear-off” slips can be processed automatically by scanning devices using Intelligent Character Recognition (ICR) technology.

TECHNOLOGY.

- ▶ Tablet PCs or “signing pads” can be used to capture digital signatures during account opening, enabling a straight-through process for new accounts; these also allow the capture of biometric characteristics to further improve fraud detection.

The database maintenance process is very similar to the initial population of the database, making it another candidate for BPO, which would alleviate the need to set up and operate a maintenance facility.

Conclusion.

To enable operational flexibility and agility and improve fraud detection, organizations are reviewing their signature verification processes and systems. Whether migrating from paper-based records, replacing existing systems, or a combination of the two, for many banks the solution is to increase visibility by implementing an enterprise-wide signature system that meets not only all of today’s requirements but provides a strategic platform for the future.

Deployment models vary from a totally in-house solution to a completely outsourced solution with several hybrid alternatives between the two.

Selecting a best-of-breed product and an experienced implementation partner will help your bank realize operational benefits today and into the future.

Unisys expertise.

Years of experience have confirmed that there is no single one-size-fits-all approach to implementing signature verification systems. Depending on your bank’s needs, the starting point could involve re-engineering a totally manual process, or integrating with systems that already provide some signature-verification functionality.

For most implementations, we have found that the approach to back-file conversion is a critical success factor and varies with each implementation. Outsourcing some or all elements of the solution may be the best approach for some organizations.

Unisys has provided the following services to clients to help them implement signature verification systems:

- ▶ Consulting, from initial feasibility and implementation strategies through to benefits realization
- ▶ Systems integration to design, build and integrate an end-to-end solution based on best-of-breed products
- ▶ Server technology and IT outsourcing to host and provide access to the central database
- ▶ Business process outsourcing (BPO) to manage the back-file conversion and on-going maintenance of the database.





Unisys has been the global distribution partner of signature verification solutions from SOFTPRO (Software Professional GmbH & Co. KG) since mid-1999.

More than 200 financial institutions—including some of the major UK and European Banks—successfully use modules of SOFTPRO's SignPlus® system, which allows for capturing and verification of both static and dynamic (biometric) signature characteristics. SOFTPRO is the world-leading signature verification solution provider. Over the past years, the company has invested about 10 million euros in further development of SignPlus® and supplied its customers with competitive advantages through increasing workflow efficiency and security.

The SignPlus® system complements the Unisys approach of deploying best-of-class solutions.

When re-engineering fraud prevention processes, our solutions can be developed and deployed using the Unisys 3D Visible Enterprise (3D-VE) methodology. Unisys 3D-VE is an innovative approach to understanding the cause and effect relationships between business vision, business operations and the information technology systems that support them, providing traceability throughout the organization.

Ultimately, 3D-VE helps our clients gain visibility into operations, anticipate future needs and reduce the risk associated with implementing new technologies.

For further information please contact:

Michael Rollitt michael.rollitt@unisys.com

Valerie Gilroy valerie.gilroy@unisys.com

About the Author.

Michael Rollitt is a manager in the UK Banking Practice at Unisys. He has managed client engagements involving application development, systems integration, installation, and support.

His areas of specialization include back-office processing, signature verification, workflow and imaging and check and remittance processing.

Michael is a Certified Project Manager and a member of the Association for Project Management.



**For more information, please visit our
website at www.unisys.com**

Specifications are subject to change without notice.

© 2005 Unisys Corporation
All rights reserved.

Unisys is a registered trademark of Unisys Corporation.
Intel is a registered trademark of Intel Corporation. Microsoft
and Windows 2000 are registered trademarks of Microsoft
Corporation. All other brands and products referenced herein
are acknowledged to be trademarks or registered trademarks
of their respective holders.

Printed in US America 06/05



4136 6667-100